

AMENDMENT
U.S. Appln. No. 10/058,189

REMARKS

Claims 1-29 are all the claims pending in the application. In response to the Office Action dated November 10, 2005, Applicant respectfully submits that pending claims 1-29 define patentable subject matter.

Applicant is filing concurrently herewith a Petition for a Three-Month Extension of time, thereby extending the time for responding to the Office Action to May 10, 2006.

The Claimed Subject Matter

By this Amendment, Applicant has made clarifying changes to the claims in order to better define the invention. The present invention relates to an encrypted message system. As defined in the present claims, a sender transmits an encrypted message to a recipient's mobile device. As discussed in the patent specification, mobile devices are often unable to provide the processing capabilities necessary to decrypt an encrypted message. According to the different claims presented herein, a message retrieval device associated with the recipient is operable to receive the encrypted message and to decrypt the encrypted message. The message retrieval device is also able to provide the decrypted message to the recipient's mobile device in a format compatible therewith.

According to other claims, the message retrieval device is able to determine, based, for example on the recipient's instructions, whether or not to decrypt the message and provide the decrypted message immediately to the recipient's mobile device or to defer encryption and instead provide the electronic message to the recipient's secure machine.

AMENDMENT
U.S. Appln. No. 10/058,189

As also described in the specification of the present application, the invention allows an encrypted message to be transmitted via a transmission medium, such as the Internet, which is not considered particularly secure, but allows a decrypted message from the recipient's message retrieval device to be transmitted to the recipient's mobile device (the path between the recipient's message retrieval device and mobile device may be considered to be an acceptable transmission medium from the standpoint of security, and therefore need not be encrypted).

The Rejections of Record

In the Office Action, claims 11-13 were rejected under 35 U.S.C. § 102(b) as being anticipated by Gordon. Claims 1 and 3-29 were rejected under 35 U.S.C. § 102(e) as being anticipated by Wright et al. Claims 1 and 2 were rejected under 35 U.S.C. § 103 as being obvious from Nelson in view of Gordon. Applicant respectfully traverses this rejection for the following reasons.

The 35 U.S.C. § 102 Rejection of Claims 11-13 based on Gordon

The Gordon patent describes a unified messaging system. As shown in Fig. 1 of Gordon, Access Nodes (UANs) are located in different geographical regions. Each UniPost Access Node provides a subscriber with an E-Mail address and account, such as an Internet address. Gordon teaches, in column 9, lines 17-33, that the UniPosts are able to encrypt transmissions between UniPost and avoid inadvertent disclosure to others. Gordon further teaches that this security is provided transparently to the sender and the receiver. Gordon also teaches that additional security may be provided on either the first or last telephone legs of the communication. For

AMENDMENT
U.S. Appln. No. 10/058,189

example, communications between a subscriber and UniPost can be encrypted in a predetermined manner, as well as the last leg of the communication path.

Gordon never addresses sending an encrypted message to a mobile device, which as described in the present specification usually does not have the processing capability to decrypt an encrypted message. That is, in Gordon, an encrypted message is intended for a device that is able to decrypt the encrypted message. As such, Gordon fails to disclose (or even remotely suggest) the claimed feature of a message retrieval device deciding based on instructions from the recipient's mobile device whether or not to decrypt the encrypted message. Rather, Gordon provides either "transparent" encryption between Nodes, or provides an encrypted message to a device that is able to decrypt the message. There is no discussion in Gordon of the recipient's mobile device instructing a message retrieval device whether or not to decrypt an encrypted message, as defined in claims 11 and 12. The claimed invention allows the user to have control over the level of security or decryption. This is very different from the Gordon system. Thus, Gordon does not disclose each and every element of claims 11 and 12, and therefore could not have anticipated these claims under 35 U.S.C. § 102. Moreover, there is absolutely no teaching in Gordon that would suggest a recipient's mobile device instructing a message retrieval device concerning whether or not to decrypt an encrypted message, as defined in claims 11 and 12. In fact, Gordon makes no mention of a user controlling security.

The 35 U.S.C. § 102 Rejection of Claims 1 and 3-29 based on Wright et al

Wright et al teaches a system for secure distribution of documents over electronic networks. Wright teaches sending an encrypted document to the recipient where it is then stored

AMENDMENT
U.S. Appl. No. 10/058,189

in the user's private data area. The user also enters all email addresses that are allowed to view the encrypted documents. Once the process is complete, emails may be provided to all of the receiving parties, informing them to go to a particular Web site to retrieve an encrypted document. (see paragraphs 0070 and 0074).

Similar to Gordon discussed above, Wright et al is not concerned with the problem addressed by the present invention wherein an encrypted message is transmitted to a recipient's mobile device which is unable to decrypt same. As discussed, mobile devices usually do not have the processing ability to decrypt an encrypted message or document. As such, mobile device are unable to view an encrypted message or document. Wright et al fails to describe sending an encrypted message to a recipient's mobile device, wherein the recipient's message retrieval device receives the encrypted message and decides whether or not to decrypt the encrypted message and send the decrypted message to the recipient's mobile device. As such, Wright does not provide each and every feature in claims 3-29 and therefore could not have anticipated these claims under 35 U.S.C. § 102. Further, since Wright is not even concerned with the problem of sending an encrypted message to a mobile device that is unable to decrypt the encrypted message, Wright does not suggest claims 3-29.

The 35 U.S.C. § 103 Rejection of Claims based on Nelson and Gordon

The Gordon patent is described above. Nelson describes a system for securing voice mail messages. It is noted that Nelson does not even send encrypted messages, as recited in claims 1 and 2. Rather, in Nelson, the process begins when a voice mail message is sent to a voice mail system 28. In response to receiving the voice mail messages, the voice mail system 28 accesses

AMENDMENT
U.S. Appln. No. 10/058,189

the appropriate public key from database 120. Nelson teaches that the received voice mail messages are then encrypted using the public key. As Nelson states:

Each incoming message is encrypted as it is received so that no unencrypted copies of the message are stored anywhere in the LAN 20. (see column 6, lines 1-40; emphasis added).

Thus, Nelson does not address the claimed invention wherein an encrypted message is transmitted to a recipient's mobile device. In Nelson, the transmitted message is not encrypted; rather, received voice messages are encrypted and then stored for later retrieval. Nelson also does teach or remotely suggest a message retrieval device that determines whether or not to decrypt an encrypted message (Nelson doesn't even receive an encrypted message) and transmit the decrypted message to the recipient's mobile device. Consequently, the combination of Nelson and Gordon would not have rendered claims 1 and 2 obvious under 35 U.S.C. § 103.

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

AMENDMENT
U.S. Appln. No. 10/058,189

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

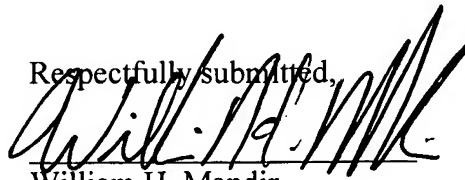
SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE

23373

CUSTOMER NUMBER

Respectfully submitted,



William H. Mandir

Registration No. 32,156

Date: May 10, 2006